

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	
	)	
Masaki OMATA	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: June 5, 2001	)	
	)	
For: USER AUTHENTICATION SYSTEM	)	
	)	
	)	
	)	
	)	

i1033 U.S. PTO  
**09/873450**  
06/05/01

**CLAIM FOR CONVENTION PRIORITY**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Japanese Patent Application No. 2000-209857

Filed: July 11, 2000

In support of this claim, enclosed is a certified copy of said prior foreign application. Said prior foreign application was referred to in the oath or declaration. Acknowledgment of receipt of the certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: June 5, 2001

By: 

Platon N. Mandros  
Registration No. 22,124

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

i1033 U.S. PTO  
09/873450  
06/05/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 7月11日

出 願 番 号

Application Number:

特願2000-209857

出 願 人

Applicant(s):

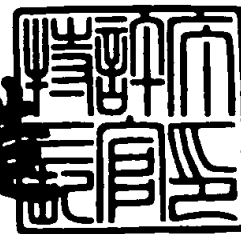
三菱電機株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 1月 5日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2000-3110200



Translation of Priority Certificate

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: July 11, 2000

Application Number: Patent Application  
No. 2000-209857

Applicant(s): MITSUBISHI DENKI KABUSHIKI KAISHA

January 5, 2001

Commissioner, Kozo Oikawa  
Patent Office

Priority Certificate No. 2000-3110200

【書類名】 特許願

【整理番号】 525497JP01

【提出日】 平成12年 7月11日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/60

【発明者】

    【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社  
社内

    【氏名】 小俣 正樹

【特許出願人】

    【識別番号】 000006013

    【氏名又は名称】 三菱電機株式会社

【代理人】

    【識別番号】 100075258

    【弁理士】

    【氏名又は名称】 吉田 研二

【選任した代理人】

    【識別番号】 100081503

    【弁理士】

    【氏名又は名称】 金山 敏彦

【選任した代理人】

    【識別番号】 100096976

    【弁理士】

    【氏名又は名称】 石田 純

【手数料の表示】

    【予納台帳番号】 001753

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

【物件名】 図面 1  
【物件名】 要約書 1  
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ユーザ認証システム

【特許請求の範囲】

【請求項 1】 音声入力機能付き通信端末装置からのログインを許可する際に、ユーザを一意に特定するユーザ識別情報及びそのユーザ識別情報に対応したパスワードに基づくユーザ認証を行うユーザ認証システムにおいて、

ユーザ識別情報と、当該ユーザが当該ユーザ識別情報を発声して得られる声紋情報とを対応付けして格納するユーザ認証データベースを有し、データ通信網を介して前記音声入力機能付き通信端末装置から送られてきたコード形式のユーザ識別情報に基づき前記ユーザ認証データベースを検索することにより特定される声紋情報と、電話回線網を介して前記音声入力機能付き通信端末装置から送られてきた音声形式によるユーザ識別情報とに基づき照合することによってユーザ認証を行うことを特徴とするユーザ認証システム。

【請求項 2】 ユーザを一意に特定するユーザ識別情報及びそのユーザ識別情報に対応したパスワードに基づくユーザ認証後に使用を許可するシステムにログイン可能な音声入力機能付き通信端末装置と、

ユーザ識別情報と、当該ユーザが当該ユーザ識別情報を発声して得られる声紋情報とを対応付けして格納するユーザ認証データベースと、

データ通信網を介して前記音声入力機能付き通信端末装置からコード形式ユーザ識別情報が送られてきたときにワンタイム識別情報を生成し、その生成したワンタイム識別情報を、データ通信網を介して前記音声入力機能付き通信端末装置へ返信すると共にそのワンタイム識別情報をパスワードとして指定したログインを不可の状態にして当該ユーザ識別情報に対応付けして前記ユーザ認証データベースへ書き込むワンタイム識別情報管理手段と、

電話回線網を介して前記音声入力機能付き通信端末装置から音声形式ユーザ識別情報が送られてきたときに、前記ユーザ認証データベースを参照することによって音声形式ユーザ識別情報に基づき声紋認証を行い、認証にパスしたときには前記ユーザ認証データベースに書き込まれている当該ワンタイム識別情報でのログインを可能状態に変更するユーザ認証処理手段と、

を有し、

前記音声入力機能付き通信端末装置は、

自通信端末装置の識別情報あるいは自通信端末装置を専用するユーザの識別情報をコード形式ユーザ識別情報として前記ワнтаイム識別情報管理手段へ送信するコード形式ユーザ識別情報送信処理手段と、

ユーザにより音声入力されたユーザ識別情報を受け付けて音声形式ユーザ識別情報として前記ユーザ認証処理手段へ送信する音声形式ユーザ識別情報送信処理手段と、

前記ユーザ認証処理手段によるユーザ認証完了後に、前記ワнтаイム識別情報管理手段から送られてきたワнтаイム識別情報を用いてシステムに自動ログインする自動ログイン処理手段と、

を有することを特徴とするユーザ認証システム。

【請求項 3】 前記ユーザ認証処理手段は、

電話回線網を介して前記音声入力機能付き通信端末装置から送られてきた音声形式ユーザ識別情報に対して音声認識処理を行うことによってコード形式でのユーザ識別情報を得る音声認識処理部と、

前記音声認識処理部により取得されたユーザ識別情報に基づいて前記ユーザ認証データベースを検索することにより特定した声紋情報と、前記音声入力機能付き通信端末装置から送られてきた音声形式ユーザ識別情報とに基づき照合を行うことで声紋認証を行う声紋認証処理部と、

有することを特徴とする請求項 2 記載のユーザ認証システム。

【請求項 4】 前記コード形式ユーザ識別情報送信処理手段は、データ通信網を介してシステムから送られてきたログイン画面を前記音声入力機能付き通信端末装置に画面表示し、そのログイン画面から入力されたユーザ名をコード形式ユーザ識別情報として前記ワнтаイム識別情報管理手段へ送信することを特徴とする請求項 2 記載のユーザ認証システム。

【請求項 5】 前記音声形式ユーザ識別情報送信処理手段は、前記ワнтаイム識別情報管理手段からデータ通信網を介してワнтаイム識別情報が送られてきた後、前記ユーザ認証処理手段から電話回線網を介して送られてきた音声ガイド

ンスに従いユーザにより入力された音声を音声形式ユーザ識別情報として前記ユーザ認証処理手段へ送信することを特徴とする請求項 2 記載のユーザ認証システム。

【請求項 6】 前記音声入力機能付き通信端末装置からのユーザログインが完了した時点で、対応するワнтаイム識別情報を前記ユーザ認証データベースから自動消去するワнтаイム識別情報削除処理手段を有することを特徴とする請求項 2 記載のユーザ認証システム。

【請求項 7】 前記音声入力機能付き通信端末装置は、インターネット機能付き携帯電話であることを特徴とする請求項 1 又は 2 記載のユーザ認証システム。

#### 【発明の詳細な説明】

【0001】

#### 【発明の属する技術分野】

本発明はユーザ認証システム、特にセキュリティ強度を維持しつつ、ログインに要するユーザ負荷の軽減を図るユーザ認証システムに関する。

【0002】

#### 【従来の技術】

ユーザ認証後に使用が許可されるシステムにおいてユーザ認証を行うための代表的な手法として、端末装置からユーザ名とパスワードを入力させる方法がある。近年では、i モード（商標）などと呼ばれるインターネット機能等を搭載したインターネット機能付き携帯電話（以下、単に「携帯電話」とも称する）の普及に伴い、社員が所持する携帯電話から企業内コンピュータへログインできるように社内システムを構築している企業は少なくない。但し、この場合、なりすましと呼ばれる第三者による社内システムへの不正侵入を防止するためにもセキュリティを確保する必要がある。セキュリティの確保のために、例えば、パスワードを長くしたり、大小英文字を混在させたりするなどパスワードを複雑にすることで、場当たりの英数文字の組合せ入力によるパスワード一致を発生しにくくしている。また、有効期間を短くするなどして見破られたパスワードの再利用を防止したりしている。



## 【 0 0 0 3 】

## 【発明が解決しようとする課題】

しかしながら、パスワードを複雑にした場合、特に英数文字を混在させた場合、数字キー以外のキーと組み合わせたモード切替操作を頻繁に行いながら携帯電話からパスワード入力をしなくてはならず、パスワード指定が極めて面倒である。機種によっては多少異なるかもしれないが、例えば、“9v”という2文字を携帯電話のキーから入力するときには、[9] [モード] [モード] [モード] [モード] [8] [8] [8] ([ ] は1回のキー操作を示す) という8回ものキー操作が必要となる。これを通常指定するパスワード長に当てはめると、携帯電話からのパスワード指定が極めて面倒なことが容易に把握できる。

## 【 0 0 0 4 】

本発明は以上のような問題を解決するためになされたものであり、その目的は、高いセキュリティ性を維持しつつユーザにかかる入力負荷を軽減させることのできるユーザ認証システムを提供することにある。

## 【 0 0 0 5 】

## 【課題を解決するための手段】

以上のような目的を達成するために、本発明に係るユーザ認証システムは、音声入力機能付き通信端末装置からのログインを許可する際に、ユーザを一意に特定するユーザ識別情報及びそのユーザ識別情報に対応したパスワードに基づくユーザ認証を行うユーザ認証システムにおいて、ユーザ識別情報と、当該ユーザが当該ユーザ識別情報を発声して得られる声紋情報とを対応付けして格納するユーザ認証データベースを有し、データ通信網を介して前記音声入力機能付き通信端末装置から送られてきたコード形式のユーザ識別情報に基づき前記ユーザ認証データベースを検索することにより特定される声紋情報と、電話回線網を介して前記音声入力機能付き通信端末装置から送られてきた音声形式によるユーザ識別情報とに基づき照合することによってユーザ認証を行うものである。

## 【 0 0 0 6 】

また、他の発明に係るユーザ認証システムは、ユーザを一意に特定するユーザ識別情報及びそのユーザ識別情報に対応したパスワードに基づくユーザ認証後に

使用を許可するシステムにログイン可能な音声入力機能付き通信端末装置と、ユーザ識別情報と、当該ユーザが当該ユーザ識別情報を発声して得られる声紋情報とを対応付けして格納するユーザ認証データベースと、データ通信網を介して前記音声入力機能付き通信端末装置からコード形式ユーザ識別情報が送られてきたときにワンタイム識別情報を生成し、その生成したワンタイム識別情報を、データ通信網を介して前記音声入力機能付き通信端末装置へ返信すると共にそのワンタイム識別情報をパスワードとして指定したログインを不可の状態にして当該ユーザ識別情報に対応付けして前記ユーザ認証データベースへ書き込むワンタイム識別情報管理手段と、電話回線網を介して前記音声入力機能付き通信端末装置から音声形式ユーザ識別情報が送られてきたときに、前記ユーザ認証データベースを参照することによって音声形式ユーザ識別情報に基づき声紋認証を行い、認証にパスしたときには前記ユーザ認証データベースに書き込まれている当該ワンタイム識別情報でのログインを可能状態に変更するユーザ認証処理手段とを有し、前記音声入力機能付き通信端末装置は、自通信端末装置の識別情報あるいは自通信端末装置を専用するユーザの識別情報をコード形式ユーザ識別情報として前記ワンタイム識別情報管理手段へ送信するコード形式ユーザ識別情報送信処理手段と、ユーザにより音声入力されたユーザ識別情報を受け付けて音声形式ユーザ識別情報として前記ユーザ認証処理手段へ送信する音声形式ユーザ識別情報送信処理手段と、前記ユーザ認証処理手段によるユーザ認証完了後に、前記ワンタイム識別情報管理手段から送られてきたワンタイム識別情報を用いてシステムに自動ログインする自動ログイン処理手段とを有するものである。

## 【 0 0 0 7 】

また、前記ユーザ認証処理手段は電話回線網を介して前記音声入力機能付き通信端末装置から送られてきた音声形式ユーザ識別情報に対して音声認識処理を行うことによってコード形式でのユーザ識別情報を得る音声認識処理部と、前記音声認識処理部により取得されたユーザ識別情報に基づいて前記ユーザ認証データベースを検索することにより特定した声紋情報と、前記音声入力機能付き通信端末装置から送られてきた音声形式ユーザ識別情報とに基づき照合を行うことで声紋認証を行う声紋認証処理部とを有するものである。

【0008】

あるいは、前記コード形式ユーザ識別情報送信処理手段は、データ通信網を介してシステムから送られてきたログイン画面を前記音声入力機能付き通信端末装置に画面表示し、そのログイン画面から入力されたユーザ名をコード形式ユーザ識別情報として前記ワнтаイム識別情報管理手段へ送信するものである。

【0009】

あるいは、前記音声形式ユーザ識別情報送信処理手段は、前記ワнтаイム識別情報管理手段からデータ通信網を介してワнтаイム識別情報が送られてきた後、前記ユーザ認証処理手段から電話回線網を介して送られてきた音声ガイダンスに従いユーザにより入力された音声を音声形式ユーザ識別情報として前記ユーザ認証処理手段へ送信するものである。

【0010】

あるいは、前記音声入力機能付き通信端末装置からのユーザログインが完了した時点で、対応するワнтаイム識別情報を前記ユーザ認証データベースから自動消去するワнтаイム識別情報削除処理手段を有するものである。

【0011】

あるいは、前記音声入力機能付き通信端末装置は、インターネット機能付き携帯電話であるものとする。

【0012】

【発明の実施の形態】

以下、図面に基づいて、本発明の好適な実施の形態について説明する。なお、本実施の形態では、本発明に係るユーザ認証システムを社内システムに適用した場合を例にして説明する。

【0013】

図1は、本発明に係るユーザ認証システムの一実施の形態を示したシステム構成図である。インターネット機能付きの携帯電話1のユーザは、携帯電話メーカーのポケット通信網を介して回線接続された相手先と対話ができるのみならず、インターネットに接続してサービス提供者が提供する各種サービスの提供を受けることができる。このとき、通常の会話を行う際には、電話番号で指定した相手

先との間に電話回線網 2 を介して回線が確立され、インターネット等を利用する際には、アドレス指定をして特定したログイン先との間にデータ通信網 3 を介して回線が確立される。なお、本実施の形態において、インターネットはデータ通信網 3 に包含され、また、携帯電話メーカのポケット通信網はデータ通信網 3 及び電話回線網 2 の双方の一部を構成するため、図 1 においては便宜的に図示していない。

## 【 0 0 1 4 】

本実施の形態における社内システムは、Webサーバ 4、データベースサーバ 5、CTI (Computer Telephony Integration)サーバ 6 及び認証サーバ 7 を LAN 8 で接続することによって構築されている。Webサーバ 4 は、携帯電話 1 からの要求に応じてサービスを提供するサーバであり、データ通信網 3 を介して携帯電話 1 とデータ通信を行う。データベースサーバ 5 は、ユーザ認証データベース 9 を管理するサーバである。CTIサーバ 6 は、コンピュータと電話とを統合させたサーバであり、電話回線網 2 を介して送られてくる携帯電話 1 からの音声認識する機能を有している。認証サーバ 7 は、声紋認証を行うためのサーバである。

## 【 0 0 1 5 】

ユーザ認証データベース 9 には、社員 ID に、当該ユーザが当該社員 ID を発声したときの声紋情報が対応付けされて予め格納されている。本実施の形態における社員 ID は、社内システムに登録されたユーザを識別するためのユーザ識別情報に相当する。携帯電話 1 を用いて社外から社内システムにアクセスするためには、その社員の声紋情報を予め登録しておく必要がある。詳細は後述するが、社員 ID には、更に認証処理において生成／消去されるワンタイム ID が対応付けして格納される。ワンタイム ID というのは、一度きりの使用が認められているパスワードである。

## 【 0 0 1 6 】

この構成において本実施の形態に含まれるワンタイム ID 管理部 10、ユーザ認証処理部 11 及びワンタイム ID 削除処理部 12 の各機能ブロックは、図 1 に示したように各サーバ 4 ～ 7 をまたいで配設される。つまり、各処理機能は、モ

ジュールを各サーバに分散配置して実現され、以下のように作用する。すなわち、ワнтаイムID管理部10は、データ通信網3を介して携帯電話1からコード形式の社員IDが送られてきたときにワнтаイムID生成し、その生成したワнтаイムIDを、データ通信網3を介して携帯電話1へ返信すると共にそのワнтаイムIDを指定したログインを不可の状態にして当該社員IDに対応付けしてユーザ認証データベース9へ書き込むが、この処理機能のうちデータベースアクセス部分の機能モジュールがデータベースサーバ5に設けられている。ユーザ認証処理部11は、CTIサーバ6に配設される音声認識処理部13と認証サーバ7に配設される声紋認証処理部14とを有している。音声認識処理部13は、電話回線網2を介して携帯電話1から送られてきた音声形式の社員IDに対して音声認識処理を行うことによってコード形式での社員IDを得る。声紋認証処理部14は、音声認識処理部13により取得された社員IDに基づいてユーザ認証データベース9を検索することにより声紋情報を特定し、その特定した声紋情報と携帯電話1から送られてきた音声形式の社員IDとに基づき照合を行うことで声紋認証を行う。そして、ユーザ認証処理部11は、認証にパスしたときにはユーザ認証データベース9に書き込まれているワнтаイムIDでのログインを可能状態に変更する。ワнтаイムID削除処理部12は、携帯電話1からのユーザログインが完了した時点で、対応するワнтаイムIDをユーザ認証データベース9から自動消去する。

#### 【0017】

一方、本実施の形態における携帯電話1には、コード形式の社員IDをCTIサーバ6に配設されているワнтаイムID管理部10へ送信するコード形式社員ID送信処理部15と、ユーザにより音声入力された社員IDを音声認識処理部13へ送信する音声形式社員ID送信処理部16と、ユーザ認証完了後にワнтаイムID管理部10から送られてきたワнтаイムIDを用いてシステムに自動ログインする自動ログイン処理部17とを有している。なお、本実施の形態のように音声入力機能付き通信端末装置が携帯電話の場合、図1に明示するまでもなく、音声形式社員ID送信処理部16は通常の電話機能として当然持っている処理機能であり、携帯電話がインターネット機能付きであればコード形式社員ID送

信処理部 1 5 も当然持っている処理機能である。なお、携帯電話 1 は、その他にも画面表示等種々の機能を有しているが、それら通常保有している機能は本実施の形態の要旨でないため説明は省略する。各サーバ 4 ～ 7 においても同様である。

#### 【 0 0 1 8 】

以上の構成を有する本実施の形態において特徴的なことは、声紋認証機能とワンタイムパスワード発行機能とを有機的に結合させたことにより、携帯電話 1 からパスワード入力のためのキー操作をさせずに社内システムにログインできるようにしたことである。本実施の形態においては、声紋情報及びワンタイムパスワードを有効に利用したことでセキュリティ強度を維持しつつユーザにかかる入力負荷を軽減することができる。

#### 【 0 0 1 9 】

次に、本実施の形態においてユーザ（社員）が携帯電話 1 から社内システムにログインしようとしたときにおける動作について図 2 及び図 3 に示したフローチャート及び図 4 に示したユーザシーンをを用いて説明する。

#### 【 0 0 2 0 】

ユーザが携帯電話 1 のインターネット機能を利用して Web サーバ 4 へアクセスすると、携帯電話 1 は、Web サーバ 4 からダウンロードされてきたログイン画面を表示する（ステップ 1 0 1）。このログイン画面の例を図 4（a）に示す。なお、このときはまだ社内システムにログインされていない状態である。ユーザは、このログイン画面から自分の社員 ID を入力し、OK ボタンを押下する。携帯電話 1 は、入力された社員 ID を受け付けると（ステップ 1 0 2）、コード形式社員 ID 送信処理部 1 5 に社員 ID を Web サーバ 4 へ送信させる。

#### 【 0 0 2 1 】

Web サーバ 4 では、送られてきた社員 ID がユーザ認証データベース 9 に登録されているかをデータベースサーバ 5 経由で確認し、もし、登録されていなければ、ログイン画面を携帯電話 1 に再度表示する（ステップ 1 0 3, 1 0 1）。一方、登録されていたときにはワンタイム ID を生成する（ステップ 1 0 4）。そして、生成したワンタイム ID をパスワードとして指定したログインを不可の

状態にして当該社員IDに対応付けしてユーザ認証データベース9へ書き込む（ステップ105）。更に、当該社員IDをユーザ名に指定したログインを不可の状態に変更する（ステップ106）。社員ID及びワнтаイムIDの各ログイン可／不可状態は、例えばフラグ情報などによりユーザ認証データベース9で保持するようにすればよい。ワнтаイムIDをパスワードに指定したログインを不可の状態にすることによってユーザ認証前においてそのワнтаイムIDによる不正なログインを防止することができる。また、本実施の形態における社員システムでは、同一ユーザに複数ログインさせないように運用しているので、社員IDをユーザ名に指定したログインを不可の状態にすることによって不正なログインを防止することができる。Webサーバ4は、その後、生成したワнтаイムIDを携帯電話1へ返信すると共に認証画面を送信する。

## 【0022】

携帯電話1は、Webサーバ4から送られてきたワнтаイムIDを内部で一時保持すると共に認証画面を表示する（ステップ107）。なお、ワнтаイムIDは画面表示しない。ユーザは、図4（b）に示した認証画面に表示されたガイダンスに従い、画面表示されたCTIサーバ6の電話番号をキー入力する。携帯電話1は、ユーザのキー入力に応じてCTIサーバ6にダイヤル発信して回線接続する。そして、ユーザ認証処理部11による声紋照合処理が開始される（ステップ108，109）。この声紋照合処理の詳細を図3に示す。

## 【0023】

CTIサーバ6と携帯電話1との回線接続後、CTIサーバ6は、社員IDを発生することを促す音声ガイダンスを携帯電話1に送る（ステップ201）。そして、ユーザは、CTIサーバ6からの音声ガイダンスに従い、社員IDを発声する。つまり、ユーザは、複雑でかつ長い文字列のパスワードをキー入力する代わりに社員IDを発声することになる。CTIサーバ6の音声認識処理部13は、ユーザにより発生された音声に対して音声認識処理を施してコード形式の社員IDを得る（ステップ202）。

## 【0024】

そして、認証サーバ7の声紋認証処理部14は、音声認識処理部13により取

得された社員ID（コード形式）に基づいてユーザ認証データベース9を検索することにより社員IDが登録されているか確認する（ステップ204）。本実施の形態では、社員IDを発声させ、それを音声認識処理することで社員IDを一意に特定することができるので、データ登録数が膨大であってもユーザ認証データベース9の検索処理を極めて迅速に行うことができる。もし、音声から得られた社員IDが登録されていないようであれば、音声ガイダンスを流してユーザに社員IDを再度発声してもらう（ステップ203，201）。ここで、社員IDが登録されていることが確認できると、その社員IDにより対応した声紋情報と、携帯電話1から送られてきた音声から得られる声紋との照合を行う（ステップ204）。照合した結果、一致したときには正しいユーザであると判断して、ユーザ認証データベース9に登録されている当該社員IDに対応したワンタイムIDのログインを可能な状態に変更する（ステップ205，206）。なお、当該社員IDでのログインは不可の状態のままである。

#### 【0025】

CTIサーバ6は、認証できたか否かの旨の音声ガイダンスをユーザに対して流した後、電話回線網2を介しての回線を切断することでユーザ認証処理を終了させる（ステップ207）。

#### 【0026】

ユーザは、認証されたことをCTIサーバ6からの音声メッセージにより確認すると、認証画面のガイダンスに従いOKボタンを押下する（ステップ108）。これにより、自動ログイン処理部17は、内部に保持しておいたワンタイムIDをWebサーバ4に送信することでシステムに自動ログインする。ユーザが正当に認証された後であれば、声紋照合処理のステップ206においてワンタイムIDでのログインが可能な状態に変更されているので、ログインすることができる。もし、ユーザ認証される前にOKボタンが押下されたとしてもワンタイムIDでのログインは不可の状態のままなのでログインをすることはできない。

#### 【0027】

Webサーバ4は、ユーザログインを確認すると、ワンタイムID削除処理部12によって、当該ユーザに対応したワンタイムIDをユーザ認証データベース



9から即座に自動消去させる（ステップ111）。これにより、そのワンタイムIDを再利用した不正ログインを未然に防止する。そして、図4（c）に例示したような社内システムのメイン画面を携帯電話1に画面表示させる（ステップ112）。なお、本実施の形態における社員システムでは、同一ユーザによる複数ログインを禁止しているので、当該社員IDでのログインは不可の状態のままである。

#### 【0028】

ユーザが社内システムの利用を終了し、ログアウトすると、CTIサーバ6は、データベースサーバ5に当該社員IDでのログインを可能な状態に変更させる（ステップ113）。

#### 【0029】

パスワードを指定した一般的なユーザ認証処理では、ユーザ名や本実施の形態の社員IDのようなユーザ識別情報と（ワンタイム）パスワードとの組合せによりユーザ照合を行う。このうちユーザ識別情報というのは、社員番号や人名、あるいはこれらの組合せなどから構成される文字列であって、ある程度の規則性があるため見破られやすい。そこで、パスワードを指定することでセキュリティの維持を図るようにしているが、セキュリティ強度を高めるためにパスワードを複雑にする必要があるが、特に携帯電話等設けるキーの数が制限されるような機器ではその指定が特に面倒になってしまう。

#### 【0030】

そこで、本実施の形態では、必ず指定しなければならないユーザ識別情報は他人に知られても良いことを前提に簡単な文字列で構成可能とし、その一方でユーザに入力指定させることのない、かつ第三者に簡単には見破られない複雑なワンタイムIDをユーザ識別情報に対応して設定し、かつパスワード指定の代わりに音声入力させ声紋認証を行うようにしたことで、ユーザは入力が簡単なユーザ識別情報を指定するだけでログインすることができる。

#### 【0031】

本実施の形態によれば、以上のようにワンタイムIDを用いることでセキュリティを維持することができ、声紋によるユーザ認証を利用することによって複雑

なパスワード指定をユーザにさせずにすむので、ログインの際に要するユーザ入力負荷を軽減することができる。

【 0 0 3 2 】

また、本実施の形態では、社員 I D でログインさせるのではなくワнтаイム I D でログインさせるようにした。これは、比較的簡単な文字列で構成される社員 I D をそのまま用いると、社員 I D による声紋認証（ステップ 2 0 5）が完了してからワнтаイム I D によるログインまで（ステップ 1 0 8）の時間の隙間に第三者が社員 I D を用いてログインできる可能性があるからである。複雑な指定が可能なワнтаイム I D を用いれば、上記隙間の時間内に第三者がワнтаイム I D を特定できる可能性が極めて低く、現実的には不可能と考えられる。更に、本実施の形態によれば、ワнтаイム I D を用いたログイン可／不可の状態を設定、保持するようにしたので、仮にワнтаイム I D を見破ったとしても不当な時間帯（つまり、ログイン不可状態が設定されている時間帯）にそのワнтаイム I D を用いてログインすることはできない。

【 0 0 3 3 】

なお、本実施の形態では、ユーザ識別情報として社員 I D を用いたが、ユーザが特定できれば、例えば、そのユーザが固有して用いる会員番号や電話番号でもよい。更に、ユーザが特定の携帯電話のみを使用する場合は、携帯電話に割り当てられている固有な情報をユーザ識別情報として使用することができる。この場合、ユーザはその携帯電話 1 の識別情報を音声により発声さえすれば何らキー入力することなくログインできることになる。

【 0 0 3 4 】

また、本実施の形態においては、音声入力機能付き通信端末装置としてインターネット機能付きの携帯電話 1 を例にして説明したが、例えば通信機能及び音声入力機能を搭載したテレフォニー端末装置やパーソナルコンピュータなどの情報端末機器でも通信機能及び音声入力機能を搭載させることで本発明を適用することができる。

【 0 0 3 5 】

【発明の効果】

本発明によれば、ユーザ識別情報とは別個に用意しかつユーザに入力指定させる必要のないワнтаイム識別情報を設定し、かつ声紋照合によるユーザ認証を行うようにしたので、セキュリティの維持を図りつつログインの際に要するユーザ入力負荷を軽減させることができる。

【0036】

特に、本発明においては、ログイン要求に応じて生成したワнтаイム識別情報を用いてのログイン可／不可の状態を設定、保持するようにしたので、ワнтаイム識別情報の生成から正当ユーザによる当該ワнтаイム識別情報を用いたログイン処理終了までのわずかな時間の隙間における不正ログインを防止することができる。

【0037】

また、ユーザログインが完了した時点で、対応するワнтаイム識別情報をユーザ認証データベースから自動消去するようにしたので、ワнтаイム識別情報を再利用した不正ログインを未然に防止することができる。

【図面の簡単な説明】

【図1】 本発明に係るユーザ認証システムの一実施の形態を示したシステム構成図である。

【図2】 本実施の形態におけるユーザ認証処理を示したフローチャートである。

【図3】 本実施の形態における声紋照合処理を示したフローチャートである。

【図4】 本実施の形態においてユーザ認証時におけるユーザシーンを示した概念図である。

【符号の説明】

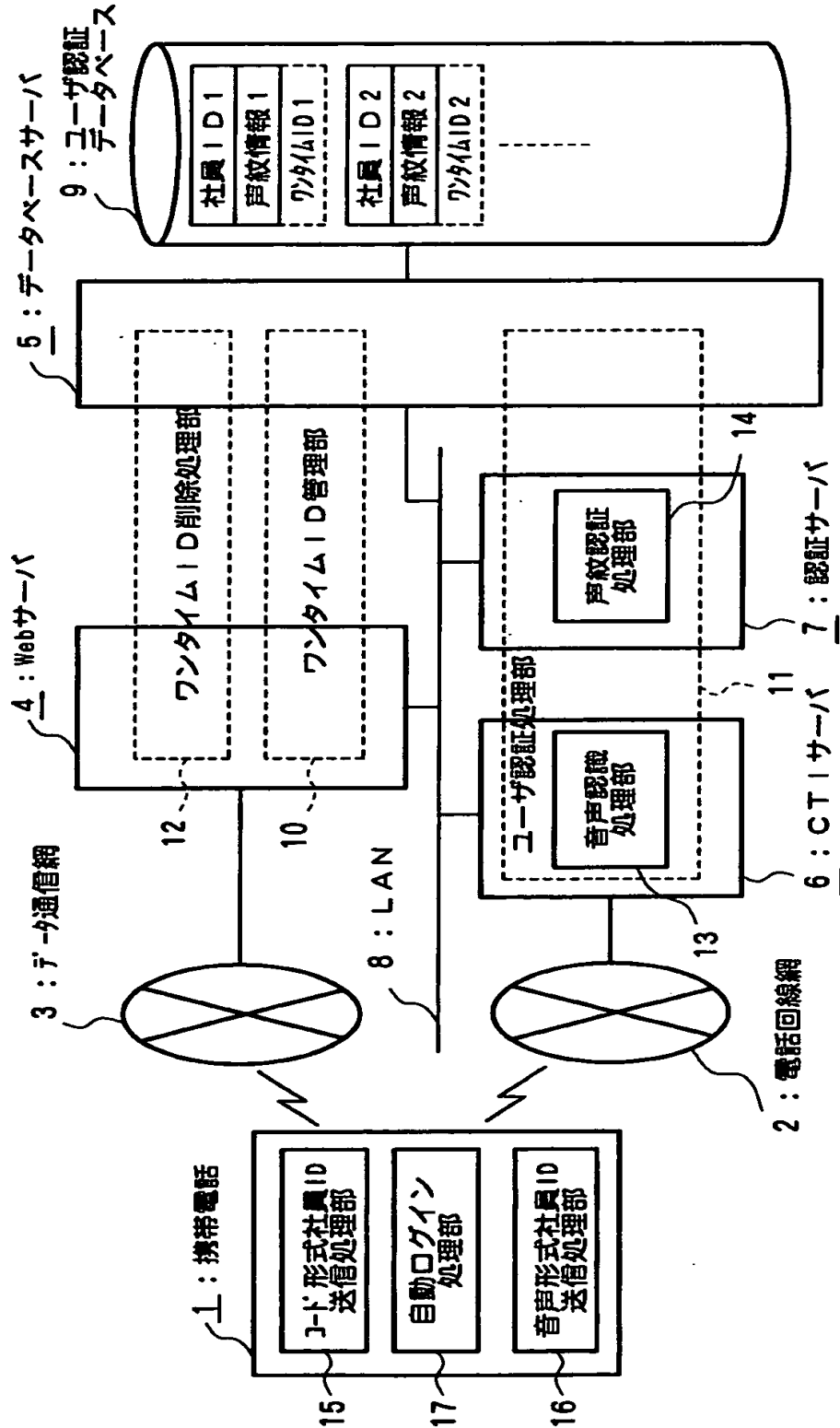
1 (インターネット機能付き) 携帯電話、2 電話回線網、3 データ通信網、4 Webサーバ、5 データベースサーバ、6 CTIサーバ、7 認証サーバ、8 LAN、9 ユーザ認証データベース、10 ワнтаイムID管理部、11 ユーザ認証処理部、12 ワнтаイムID削除処理部、13 音声認識処理部、14 声紋認証処理部、15 コード形式社員ID送信処理部、16

特 2 0 0 0 - 2 0 9 8 5 7

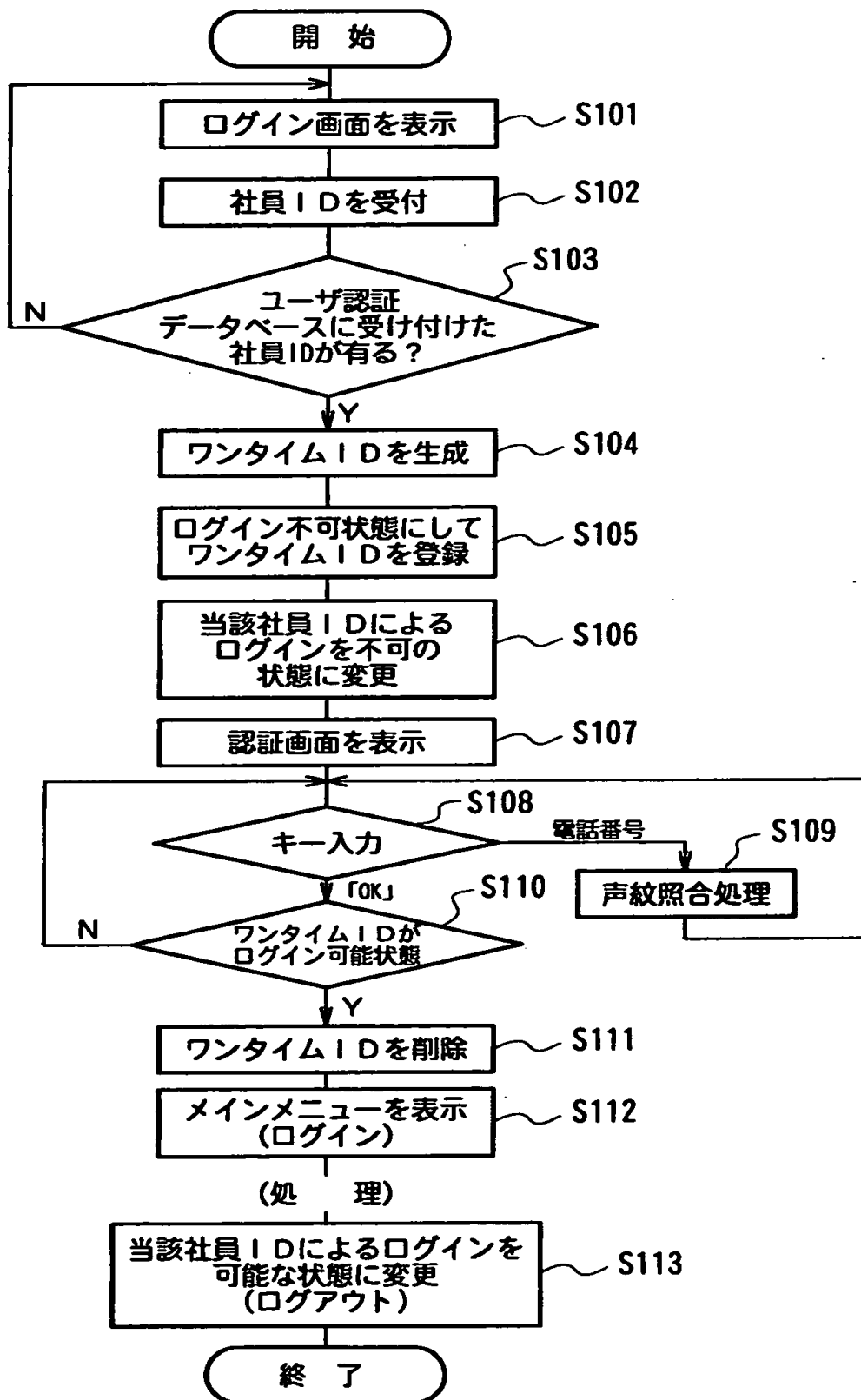
音声形式社員 I D 送信処理部、 1 7 自動ログイン処理部。

【書類名】 図面

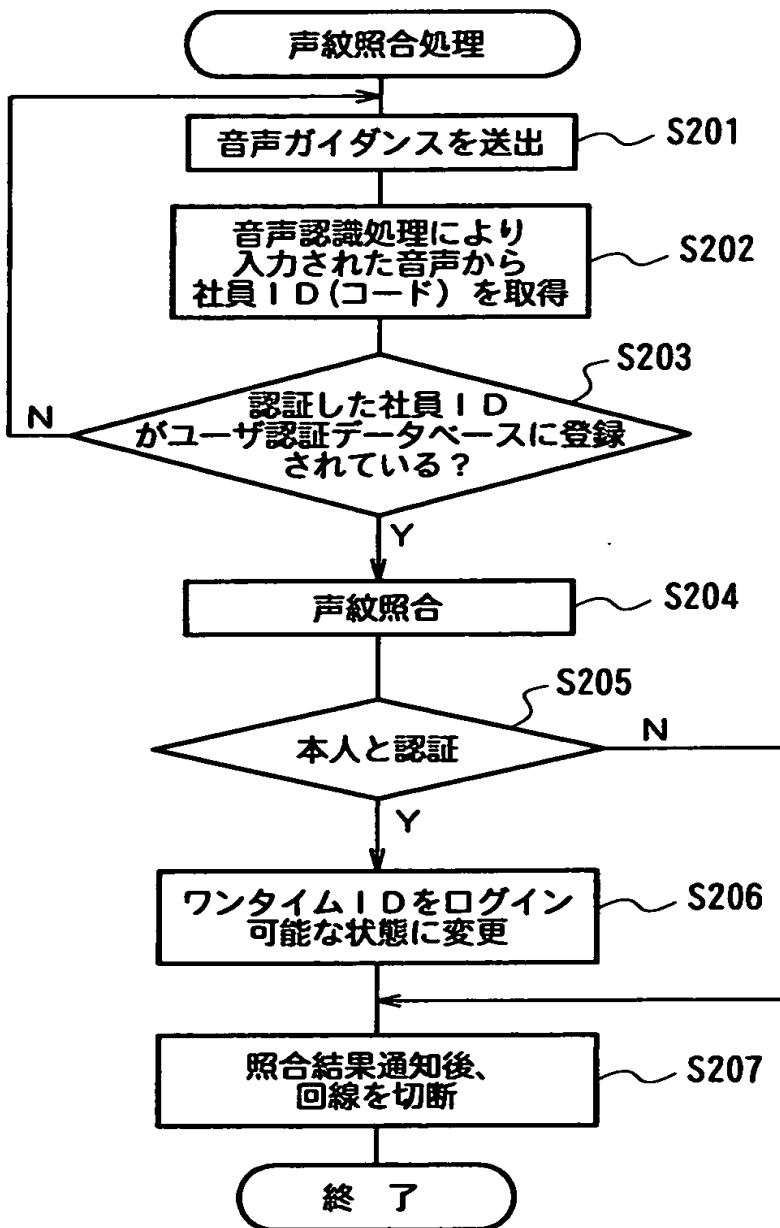
【図 1】



【図 2】

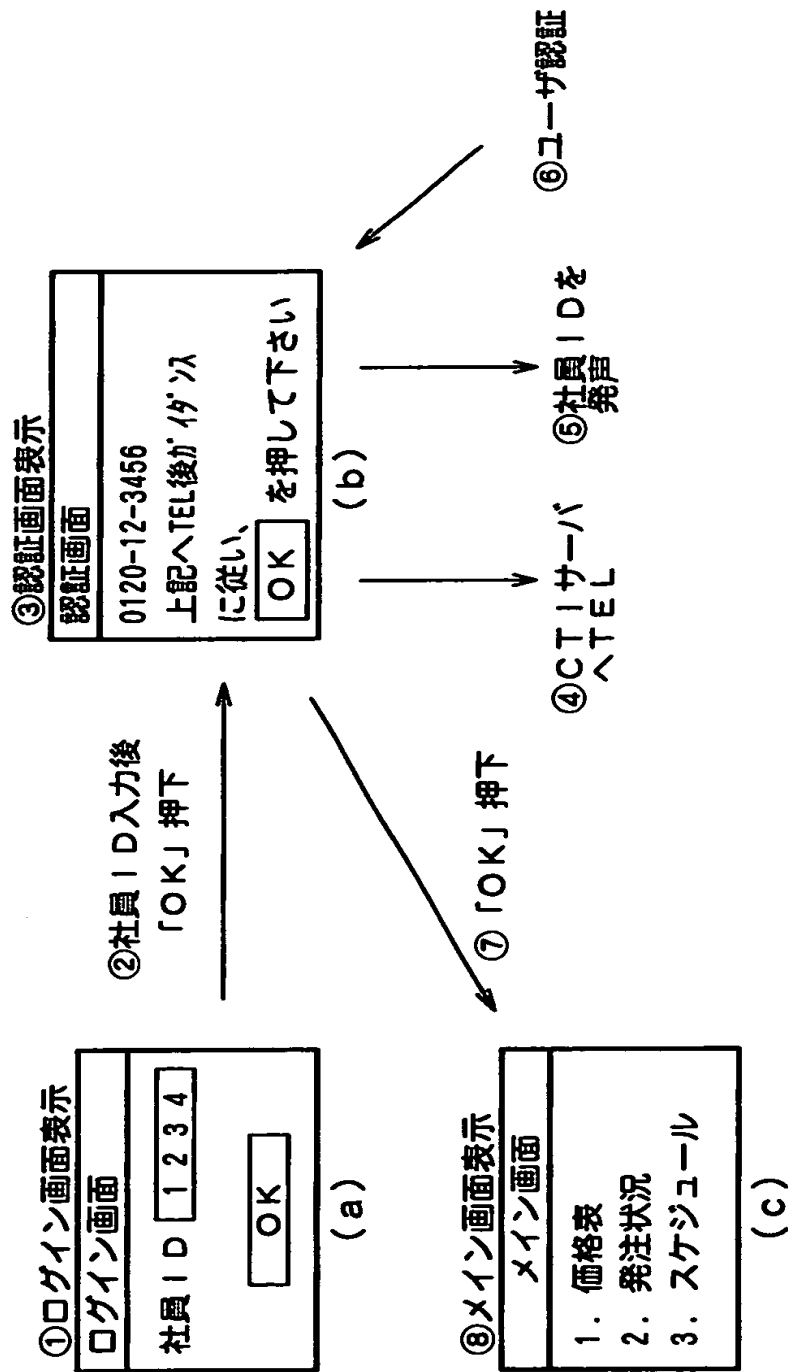


【図 3】



【図4】

ユーザーマシン





【書類名】 要約書

【要約】

【課題】 高いセキュリティ性を維持しつつユーザにかかる入力負担を軽減させる。

【解決手段】 社員IDに、当該ユーザが当該社員IDを発声したときの声紋情報を対応付け格納したユーザ認証データベース9を設ける。Webサーバ4は、データ通信網3を介して携帯電話1から社員IDを指定したログイン要求があると、ワンタイムIDをログイン不可状態で生成し、社員IDに対応付けしてユーザ認証データベース9に登録すると共にワンタイムIDを携帯電話1へ返信する。CTIサーバ6は、電話回線網2を介した回線接続後、社員IDをユーザに発声させ音声認識処理を行う。認証サーバ7は、音声認識された社員IDに対応した声紋情報と発声された社員IDとの声紋照合を行い、認証できたときにワンタイムIDをログイン可状態に変更する。携帯電話1は、ユーザ認証後ワンタイムIDをCTIサーバ6へ送信して自動ログインする。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000006013]

1. 変更年月日 1990年 8月24日

[変更理由] 新規登録

住 所 東京都千代田区丸の内2丁目2番3号  
氏 名 三菱電機株式会社